DETAILED ACTION

Response to Amendment

1. In response to communications filed on 02/07/2008, the Examiner acknowledges the amendments made to the claims and have both considered and applied them to the claims.

This Office Action reflects the amendments made with communications filed 02/07/2008, but not reflected in the Office Action response dated 04/28/2008. In this Action the amendments to the claims have been applied and are addressed as detailed below.

Claims 1-11 are presented for examination.

Response to Remarks/Arguments

1.1 Applicant's arguments, with respect to the rejection of claims 1-11 have been fully considered but they are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malinen et al. (U.S. Patent Application Publication No. 2005/0078824 A1) in view of Quick ("Common Security Algorithms" - 3rd Generation Partnership Project 2. Qualcomm Incorporated, July 10, 2002,).

Regarding claims 1 and 11, Malinen et al., discloses a method of authenticating a user identity module implemented in an access terminal, comprising:
Receiving, at the access terminal and over an air interface, a first challenge associated with a first authentication process (0075 – "On receiving the message the AS first identifies the AuC holding the authentication information for the user. (this first identification is equated to the first authentication" and "[Access Server (AS)] creates the Extensible Access protocol (EAP) Request/AKA/Challenge message containing the AT_RAND value, the AT_AUTN value, and the AT_MAC value") is equated to the first challenge; deriving, at the access terminal, a second challenge associated with a second authentication process based on at least a portion of the first challenge (0075 – "[Access Server (AS) creates and] sends a message, containing the EAP Request/AKA/Challenge message in it and the NAI identifying the user (in the User-Name attribute), to the AC.") is equated to the second challenge; performing, at the user identity module, the second authentication process using the derived second challenge and producing at least one authentication parameter therefrom (0077 – "When the terminal receives this message, it first extracts the EAP Request/AKA/Challenge

message. It then uses the AKA to calculate the AT_RES values, giving the AT_RAND and AT_MAC values received inside the EAP Request/AKA/Challenge as input to the AKA. It also calculates the AT_AUTN value and compares it to the AT_AUTN received in the EAP Request/AKA/Challenge. If these values match, the EAP Request/AKA/Challenge message is authenticated successfully.");
Deriving, at the access terminal, a key associated with the first authentication process based on the at least one authentication parameter (0056 – "Several authentication mechanisms may be used. In the following description of the preferred embodiments, EAP-AKA (Authentication and Key Agreement) authentication mechanism using USIM (Universal Subscriber Identity Module) (first embodiment) and an authentication mechanism using R-UIM (removable user identity module) applying a CAVE (Cellular Authentication and Voice Encryption) algorithm (second embodiment) are taken as examples").

Malinen et al. is silent in disclosing performing an authentication using the RAND challenge to produce a SMEKEY and a PLCM (0152-0154 and 0147-0157); and deriving a secret CHAP key based on the SMEKEY and PLCM., however Malinen et al. does disclose "an authentication mechanism using ... a Cellular Authentication and Voice Encryption (CAVE) algorithm, or a USIM applying te AKA algorithm (0030-0031)," this disclosure in combination with the Quick

disclosure of, creating "the CDMA private long code mask (PLCM) and the message encryption key CMEAKEY for intersystem handoff from a system using AKA to a system using older (2G) algorithms for authentication and privacy. (On the ANS-41 network, these keys are referred to as CDMA_PLCM and SMEKEY.) "(Quick page 9). It would have been obvious for one of ordinary skill in the art to have modified the disclosed CDMA private long code mask (PLCM) and the message encryption key CMEAKEY of Quick into the SMEKEY and PLCM of the instant application because these terminologies are used interchangeably.

Regarding claim 2, Malinen et al., discloses a method, as set forth in claim 1, wherein receiving the first challenge associated with the first authentication process further comprises receiving a CHAP challenge (0152 – "packet data sessions via a PDSN, as is currently done with EAP-CHAP").

Regarding claim 3, Malinen et al., discloses a method, as set forth in claim 2, wherein deriving the second challenge associated with the second authentication process based on at least a portion of the first challenge further comprises deriving a RAND challenge based on at least a portion of the CHAP challenge ("[Access Server (AS)] creates the Extensible Access protocol (EAP) Request/AKA/Challenge message containing the AT_RAND value, the AT_AUTN value, and the AT_MAC value") is equated to the first challenge and "a message, containing the EAP Request/AKA/Challenge message in it and the

NAI identifying the user (in the User-Name attribute), to the AC.") is equated to the second challenge).

Regarding claim 4, Malinen et al., discloses a method, as set forth in claim 3, wherein deriving the RAND challenge based on at least a portion of the CHAP challenge further comprises deriving the RAND challenge from a selected number of least significant bits in the CHAP challenge (0152-0154).

Regarding claim 5, Malinen et al., discloses a method, as set forth in claim 4, wherein performing the second authentication process using the derived second challenge and producing at least one authentication parameter therefrom further comprises performing a CAVE based authentication process on the RAND challenge to produce SMEKEY (0030, 0056, 0144-146 and rejected the same rationale as claim 1).

Regarding claim 6, Malinen et al., discloses a method, as set forth in claim 5 wherein performing the CAVE based authentication process on the RAND challenge to produce SMEKEY further comprises performing the CAVE based authentication process on the RAND challenge to produce SMEKEY and PLCM. (Rejected under the same rationale as claim 1).

Regarding claim 7, Malinen et al., discloses a method, as set forth in claim 6, wherein deriving the key associated with the first authentication process based on the at least one authentication parameter further comprises deriving the key associated with the first authentication process based on SMEKEY and PLCM (Rejected under the same rationale as claim 1).

Regarding claim 8, Malinen et al., discloses a method, as set forth in claim 1, further comprising: generating, at the access terminal, an authentication response based on the key and delivering the authentication response over the air interface to a network to request access to the network (0056-0060).

Regarding claim 9, Malinen et al., discloses a method, as set forth in claim 8, further comprising: determining that the first challenge associated with the first authentication process is a re-authentication challenge (0073-0074); bypassing the derivation of the second challenge associated with the second authentication process based on at least a portion of the first challenge in response to the determining that the first challenge is the re-authentication challenge (0075); bypassing the performance of the second authentication process using the derived second challenge and producing at least one authentication parameter therefrom in response to the determining that the first challenge is the re-authentication challenge (0076-0079).

Malinen et al. is silent in disclosing the key associated with the first authentication process based on the at least one authentication parameter further comprises using a previously derived key in response to the determining that the first challenge is the re-authentication challenge (0056-0060 of Malinen et al.).

Regarding claim 10, Malinen et al., discloses a method, as set forth in claim 8, further comprising: determining that the first challenge associated with the first authentication process is a re-authentication challenge (0073-0074); and wherein delivering the key to a network to request access to the network further comprises delivering a previously derived key in response to the determining that the first challenge is the re-authentication challenge (0076-0079).

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHINWENDU C. OKORONKWO whose telephone number is (571)272-2662. The examiner can normally be reached on MWF 2:30 - 6:00, TR 9:00-3:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. C. O./

Examiner, Art Unit 2136

April 24, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136